

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LA MÉTHODE

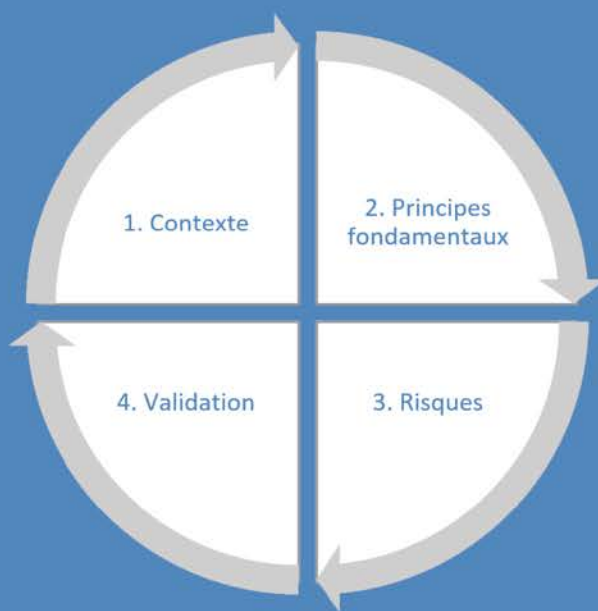


Table des matières

| | |
|--|----------|
| Avant-propos | 1 |
| Introduction | 2 |
| Comment mener un PIA ? | 3 |
| 1 Étude du contexte | 4 |
| 1.1 Vue d'ensemble | 4 |
| 1.2 Données, processus et supports | 4 |
| 2 Étude des principes fondamentaux | 5 |
| 2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement..... | 5 |
| 2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées . | 5 |
| 3 Étude des risques liés à la sécurité des données | 6 |
| Qu'est-ce qu'un risque sur la vie privée ? | 6 |
| 3.1 Évaluation des mesures existantes ou prévues | 7 |
| 3.2 Appréciation des risques : les atteintes potentielles à la vie privée | 7 |
| 4 Validation du PIA | 8 |
| 4.1 Préparation des éléments utiles à la validation | 8 |
| 4.2 Validation formelle..... | 8 |
| Annexes | 9 |
| Définitions | 9 |
| Références bibliographiques..... | 10 |
| Couverture des critères des [LignesDirectrices-G29]..... | 11 |

Avant-propos

La méthode de la CNIL est composée de trois guides, décrivant respectivement la démarche, des modèles utiles pour formaliser l'étude et des bases de connaissances (un catalogue de mesures destinées à respecter les exigences légales et à traiter les risques, et des exemples) utiles pour mener l'étude :

Ils sont téléchargeables sur le site de la CNIL :



<https://www.cnil.fr/fr/PIA-privacy-impact-assessment>

Conventions d'écriture pour l'ensemble de ces documents :

- ❑ le terme « **vie privée** » est employé comme raccourci pour évoquer l'ensemble des libertés et droits fondamentaux (notamment ceux évoqués dans le [\[RGPD\]](#), par les articles 7 et 8 de la [\[Charte-UE\]](#) et l'article 1 de la [\[Loi-I&L\]](#) : « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ») ;
- ❑ l'acronyme « **PIA** » est utilisé pour désigner indifféremment *Privacy Impact Assessment*, étude d'impact sur la vie privée (EIVP), analyse d'impact relative à la protection des données, et *Data Protection Impact Assessment* (DPIA) ;
- ❑ les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

Introduction

Ce guide explique comment mener une "analyse d'impact relative à la protection des données" (cf. art. 35 du [\[RGPD\]](#)), plus communément appelée *Privacy Impact Assessment* (PIA).

Il décrit la manière d'employer la méthode [\[EBIOS\]](#)¹ dans le contexte spécifique « Informatique et libertés ». La démarche est conforme aux critères des [\[LignesDirectrices-G29\]](#) (voir la démonstration de couverture fournie en annexe) et compatible avec les normes internationales relatives à la gestion des risques (ex : [ISO 31000]).

Le fonctionnement itératif de cette méthode doit permettre de garantir une utilisation raisonnée et fiable de données à caractère personnel dans le cadre de leur traitement.

La méthode ne traite ni des conditions en amont déterminant s'il faut mener un PIA (cf. art. 35.1 du [\[RGPD\]](#)) ni de celles en aval déterminant qu'il faut consulter l'autorité de protection des données (cf. art. 36.1 du [\[RGPD\]](#)).

Théoriquement mené par un responsable de traitement, un PIA a pour objectif de construire et de démontrer la mise en œuvre des principes de protection de la vie privée afin que les personnes concernées conservent la maîtrise de leurs données à caractère personnel.

Ce guide s'adresse aux responsables de traitements qui souhaitent justifier de leur démarche de conformité et des mesures qu'ils ont choisies (notion de responsabilité ou d'*accountability* en anglais, cf. art. 25 du [\[RGPD\]](#)), ainsi qu'aux fournisseurs de produits qui souhaitent démontrer que leurs solutions sont conçues dans une logique de conception respectueuse de la vie privée (notion de *Privacy by Design* en anglais, cf. art. 25 du [\[RGPD\]](#))². Il est utile à toutes les parties prenantes dans la création ou l'amélioration de traitements de données à caractère personnel ou de produits :

- ❑ les autorités décisionnaires, qui commanditent et valident la création de nouveaux traitements de données à caractère personnel ou produits ;
- ❑ les maîtrises d'ouvrage, qui doivent apprécier les risques pesant sur leur système et donner des objectifs de sécurité ;
- ❑ les maîtrises d'œuvre, qui doivent proposer des solutions pour traiter les risques conformément aux objectifs identifiés par les maîtrises d'ouvrage ;
- ❑ les correspondants « informatique et libertés » ou délégués à la protection des données, qui doivent accompagner les maîtrises d'ouvrage et les autorités décisionnaires dans la protection des données à caractère personnel ;
- ❑ les responsables de la sécurité des systèmes d'information, qui doivent accompagner les maîtrises d'ouvrage dans le domaine de la sécurité des systèmes d'information.

¹ EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – est la méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

² Dans la suite du document, le terme « traitement de données à caractère personnel » est interchangeable avec le terme « produit ».

Comment mener un PIA ?

La démarche de conformité mise en œuvre en menant un PIA repose sur deux piliers :

1. **les principes et droits fondamentaux**³, « non négociables », qui sont fixés par la loi et doivent être respectés, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
2. **la gestion des risques sur la vie privée**⁴, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données⁵.



Figure 1 – La démarche de conformité à l'aide d'un PIA

En résumé, pour mener un PIA, il convient de :

1. délimiter et décrire le **contexte** du(des) traitement(s) considéré(s) ;
2. analyser les mesures garantissant le respect des **principes fondamentaux** : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
3. apprécier les **risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;
4. formaliser la **validation** du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

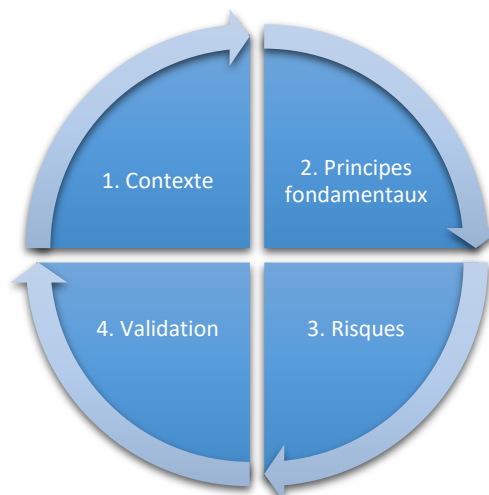


Figure 2 – Démarche générale pour mener un PIA

Il s'agit d'un processus d'amélioration continue. Il requiert donc parfois plusieurs itérations pour parvenir à un dispositif de protection de la vie privée acceptable. Il requiert en outre une surveillance des évolutions dans le temps (du contexte, des mesures, des risques, etc.), par exemple tous les ans, et des mises à jour dès qu'une évolution significative a lieu.


La démarche devrait être employée dès la conception d'un nouveau traitement de données à caractère personnel. En effet, une application en amont permet de déterminer les mesures nécessaires et suffisantes, et donc d'optimiser les coûts. A contrario, une application tardive, alors que le système est déjà créé et les mesures en place, peut remettre en question les choix effectués.


³ Finalité déterminée, explicite et légitime ; données adéquates, pertinentes et non excessives ; information claire et complète des personnes ; durée de conservation limitée ; droit d'opposition, d'accès, de rectification et suppression, etc.

⁴ Liés à la sécurité des données à caractère personnel et ayant un impact sur la vie privée des personnes concernées.

⁵ Afin de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès » (article 34 de la [Loi-I&L](#)).

1 Étude du contexte

 Généralement réalisée par la maîtrise d'ouvrage⁶, avec l'aide d'une personne en charge des aspects « Informatique et libertés »⁷.

 Objectif : obtenir une vision claire des traitements de données personnelles considérés.

1.1 Vue d'ensemble

- ❑ Présenter le **traitement** considéré, sa **nature**, sa **portée**, son **contexte**, ses **finalités** et ses **enjeux**⁸ de manière synthétique.
- ❑ Identifier le **responsable du traitement** et les éventuels **sous-traitants**.
- ❑ Recenser les **référentiels applicables** au traitement, utiles ou à respecter⁹, notamment les codes de conduite approuvés (cf. art. 40 du [\[RGPD\]](#)) et certifications en matière de protection des données (cf. art. 42 du [\[RGPD\]](#))¹⁰.

1.2 Données, processus et supports

- ❑ Délimiter et décrire le périmètre de manière détaillée :
 - les **données** personnelles concernées, leurs **destinataires** et **durées de conservation** ;
 - une description des **processus** et des **supports** de données pour l'ensemble du cycle de vie des données (depuis leur collecte jusqu'à leur effacement).

⁶ Il s'agit des métiers. Elle peut être déléguée, représentée ou sous-traitée.


⁷ Correspondant Informatique et libertés, délégué à la protection des données, ou autre.

⁸ Répondre à la question « Quels sont les bénéfices attendus (pour l'organisme, pour les personnes concernées, pour la société en général...) ? ».

⁹ Selon les cas, ils serviront notamment à démontrer le respect de principes fondamentaux, à justifier des mesures ou à prouver qu'elles correspondent à l'état de l'art.

¹⁰ Autres exemples : politique de sécurité, normes juridiques sectorielles, etc.

2 Étude des principes fondamentaux

 Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge des aspects « Informatique et libertés ».

 **Objectif** : bâtir le dispositif de conformité aux principes de protection de la vie privée.

2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

- ❑ Expliciter et justifier les **choix effectués pour respecter les exigences** suivantes :
 1. **finalité(s)** : déterminée, explicite et légitime (cf. art. 5.1 (b) du [\[RGPD\]](#)) ;
 2. **fondement** : licéité du traitement, interdiction du détournement de finalité (cf. art. 6 du [\[RGPD\]](#))¹¹ ;
 3. **minimisation des données** : adéquates, pertinentes et limitées (cf. art. 5.1 (c) du [\[RGPD\]](#))¹² ;
 4. **qualité des données** : exactes et tenues à jour (cf. art. 5.1 (d) du [\[RGPD\]](#)) ;
 5. **durées de conservation** : limitées (cf. art. 5.1 (e) du [\[RGPD\]](#)).
- ❑ Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément au [\[RGPD\]](#).
- ❑ Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées

- ❑ Identifier ou déterminer, et décrire, les **mesures retenues** (existantes ou prévues) **pour respecter les exigences** suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre) :
 1. **information** des personnes concernées (traitement loyal et transparent, cf. art. 12, 13 et 14 du [\[RGPD\]](#)) ;
 2. **recueil du consentement**, le cas échéant¹³ : exprès, démontrable, retirable (cf. art. 7 et 8 du [\[RGPD\]](#)) ;
 3. exercice des **droits d'accès et à la portabilité** (cf. art. 15 et 20 du [\[RGPD\]](#)) ;
 4. exercice des **droits de rectification et d'effacement** (cf. art. 16 et 17 du [\[RGPD\]](#)) ;
 5. exercice des **droits de limitation du traitement et d'opposition** (cf. art. 18 et 21 du [\[RGPD\]](#)) ;
 6. **sous-traitance** : identifiée et contractualisée (cf. art. 28 du [\[RGPD\]](#)) ;
 7. **transferts** : respect des obligations en matière de transfert de données en dehors de l'Union européenne (cf. art. 44 à 49 du [\[RGPD\]](#)).
- ❑ Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément au [\[RGPD\]](#).
- ❑ Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

¹¹ Démontrer également que les destinataires sont légitimes.

¹² Démontrer également que les destinataires ont réellement besoin d'accéder aux données.

¹³ Justifier les cas où le consentement n'est pas obtenu.

3 Étude des risques liés à la sécurité des données¹⁴

Qu'est-ce qu'un risque sur la vie privée ?

Un risque est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne. Plus précisément, il décrit :

- ❑ comment des sources de risques (ex. : un salarié soudoyé par un concurrent)
- ❑ pourraient exploiter les vulnérabilités des supports de données (ex. : le système de gestion des fichiers, qui permet de manipuler les données)
- ❑ dans le cadre de menaces (ex. : détournement par envoi de courriers électroniques)
- ❑ et permettre à des événements redoutés de survenir (ex. : accès illégitime à des données)
- ❑ sur les données à caractère personnel (ex. : fichier des clients)
- ❑ et ainsi provoquer des impacts sur la vie privée des personnes concernées (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels).

Le schéma suivant synthétise l'ensemble des notions présentées :

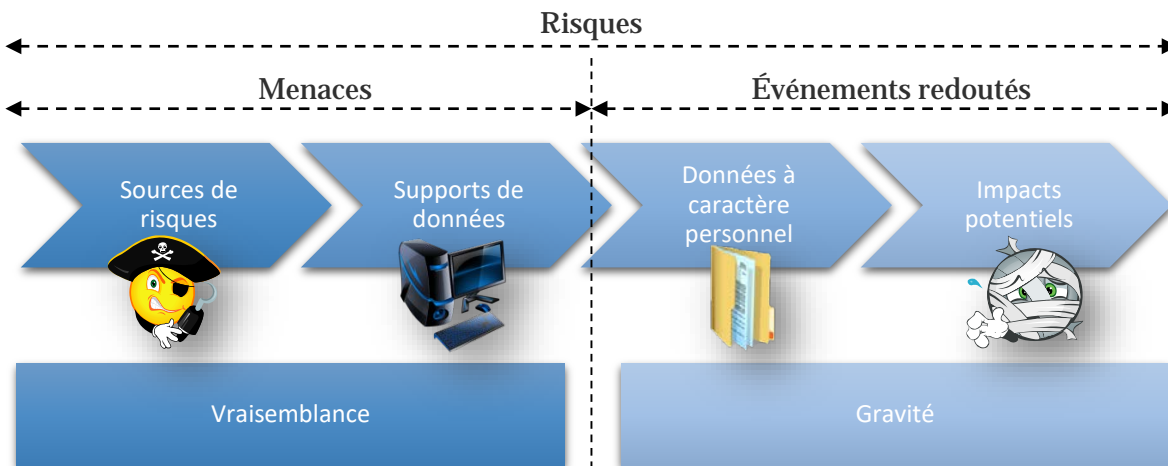


Figure 3 – Éléments composant les risques

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- ❑ la **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels¹⁵ ;
- ❑ la **vraisemblance** traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

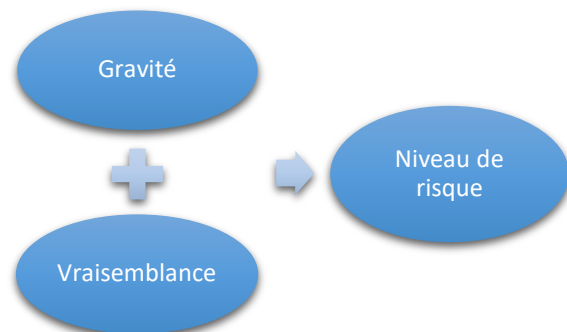



Figure 4 – Éléments permettant d'estimer les risques

¹⁴ Cf. art. 32 du [\[RGPD\]](#).

¹⁵ Compte tenu du contexte (nature des données, personnes concernées, finalité du traitement, etc.).


3.1 Évaluation des mesures existantes ou prévues


 Généralement réalisé par la maîtrise d'œuvre¹⁶, puis évaluée par une personne en charge de la sécurité de l'information¹⁷.

 **Objectif** : obtenir une bonne connaissance des mesures contribuant à la sécurité.

- ❑ Identifier ou déterminer les **mesures existantes ou prévues** (déjà engagées), qui peuvent être de trois natures différentes :
 1. **mesures portant spécifiquement sur les données du traitement** : chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, etc. ;
 2. **mesures générales de sécurité du système dans lequel le traitement est mis en œuvre** : sécurité de l'exploitation, sauvegardes, sécurité des matériels, etc. ;
 3. **mesures organisationnelles (gouvernance)** : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, etc.
- ❑ Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité.
- ❑ Le cas échéant, préciser leur description ou proposer des mesures complémentaires.

3.2 Appréciation des risques : les atteintes potentielles à la vie privée

 Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge de la sécurité de l'information.

 **Objectif** : obtenir une bonne compréhension des causes et conséquences des risques.

- ❑ Pour chaque événement redouté (un accès illégitime à des données¹⁸, une modification non désirée de données¹⁹, et une disparition de données²⁰) :
 1. déterminer les **impacts** potentiels sur la vie privée des personnes concernées s'ils survenaient²¹ ;
 2. estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
 3. identifier les **menaces** sur les supports des données qui pourraient mener à cet événement redouté²² et les **sources de risques** qui pourraient en être à l'origine ;
 4. estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier.
- ❑ Déterminer si les risques ainsi identifiés²³ peuvent être jugés acceptables compte tenu des mesures existantes ou prévues.
- ❑ Dans la négative, proposer des mesures complémentaires et ré-estimer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels.

¹⁶ Elle peut être déléguée, représentée ou sous-traitée.

¹⁷ Responsable de la sécurité des systèmes d'information ou autre.

¹⁸ Elles sont connues de personnes non autorisées (atteinte à la confidentialité des données).

¹⁹ Elles ne sont plus intègres ou sont changées (atteinte à l'intégrité des données).


²⁰ Elles ne sont pas ou plus disponibles (atteinte à la disponibilité des données).


²¹ Répondre à la question « Que craint-on qu'il arrive aux personnes concernées ? ».

²² Répondre à la question « Comment cela pourrait-il arriver ? ».

²³ Un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne.

4 Validation du PIA

 Généralement réalisée par le responsable de traitement, avec l'aide d'une personne en charge des aspects « Informatique et libertés ».

 **Objectif** : décider d'accepter ou non le PIA au regard des résultats de l'étude.

4.1 Préparation des éléments utiles à la validation

- Consolider et mettre en forme les résultats de l'étude :
 1. élaborer une représentation visuelle des **mesures choisies pour respecter les principes fondamentaux**, en fonction de leur conformité au [\[RGPD\]](#) (ex : à améliorer, ou jugé comme conforme) ;
 2. élaborer une représentation visuelle des **mesures choisies pour contribuer à la sécurité des données**, en fonction de leur conformité aux bonnes pratiques de sécurité (ex : à améliorer, ou jugé comme conforme) ;
 3. élaborer une cartographie visuelle des **risques résiduels**²⁴ en fonction de leur gravité et vraisemblance ;
 4. élaborer un **plan d'action** à partir des mesures complémentaires identifiées lors des étapes précédentes : pour chaque mesure, déterminer au moins le responsable de sa mise en œuvre, son coût (financier et/ou en termes de charge) et son échéance prévisionnelle.
- Formaliser la prise en compte des parties prenantes :
 1. le **conseil de la personne en charge des aspects « Informatique et libertés »**, si elle a été désignée (cf. art. 35 (2) du [\[RGPD\]](#)) ;
 2. l'**avis des personnes concernées ou de leurs représentants**, le cas échéant (cf. art. 35 (9) du [\[RGPD\]](#)).

4.2 Validation formelle

- Décider de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes. Le PIA peut ainsi être :
 1. validé ;
 2. à améliorer (expliquer en quoi) ;
 3. refusé (ainsi que le traitement considéré).
- Le cas échéant, revoir les étapes précédentes pour que le PIA puisse être validé.

²⁴ Risques qui subsistent après application des mesures.

Annexes

Définitions

Note : les libellés entre parenthèses correspondent aux libellés courts employés dans ce document.

| | |
|--|---|
| Donnée à caractère personnel (donnée) | <p>Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. [RGPD]</p> <p><i>Note : pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. [Loi-I&L]</i></p> |
| Événement redouté | <p>Violation potentielle de données pouvant mener à des impacts sur la vie privée des personnes concernées.</p> |
| Gravité | <p>Estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées.</p> <p><i>Note : elle dépend essentiellement du caractère préjudiciable des impacts potentiels.</i></p> |
| Menace | <p>Mode opératoire composé d'une ou plusieurs actions unitaires sur des supports de données.</p> <p><i>Note : elle est utilisée, volontairement ou non, par des sources de risques, et peut provoquer un événement redouté.</i></p> |
| Mesure | <p>Action à entreprendre.</p> <p><i>Note : elle peut être technique ou organisationnelle, et peut consister mettre en œuvre des principes fondamentaux ou à éviter, réduire, transférer ou prendre tout ou partie des risques.</i></p> |
| Personnes concernées | <p>Personnes auxquelles se rapportent les données qui font l'objet du traitement. [Loi-I&L]</p> |
| Responsable de traitement | <p>La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. [RGPD]</p> <p><i>Note : sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement. [Loi-I&L]</i></p> |
| Risque | <p>Scénario décrivant un événement redouté et toutes les menaces qui le rendent possibles.</p> |

Note : il est estimé en termes de gravité et de vraisemblance.

Source de risque Personne ou source non humaine qui peut être à l'origine d'un risque.

Note : elle peut agir de manière accidentelle ou délibérée.

Support de données Bien sur lequel reposent des données.

Note : il peut s'agir de matériels, de logiciels, de canaux informatiques, de personnes, de supports papier ou de canaux de transmission papier.

Traitement de données à caractère personnel (traitement) Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. [\[RGPD\]](#)

Vraisemblance Estimation de la possibilité qu'un risque se réalise.

Note : elle dépend essentiellement des vulnérabilités exploitables et des capacités des sources de risques à les exploiter.

Références bibliographiques

[\[Charte-UE\]](#) Charte des droits fondamentaux de l'Union européenne, 2010/C 83/02.

[\[RGPD\]](#) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[\[Loi-I&L\]](#) Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée²⁵.

[\[LignesDirectrices-G29\]](#) Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rév. 01, Groupe de travail « Article 29 » sur la protection des données.

[\[EBIOS\]](#) Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques, ANSSI.

[\[ISO 31000\]](#) ISO 31000:2009, Management du risque – Principes et lignes directrices, ISO.

²⁵ Modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et par la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.

Couverture des critères des [LignesDirectrices-G29]

| Critères des [LignesDirectrices-G29] (et références au [RGPD]) | Couverture | Chapitre de ce guide |
|---|------------|---|
| <p>Une description systématique du traitement est fournie (Article 35(7)(a)) :</p> <ul style="list-style-type: none"> - la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90) ; - les données à caractère personnel, destinataires et durée de conservation sont recensés ; - une description fonctionnelle du traitement est fournie ; - les biens sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, papier ou canaux de transmission papier) sont identifiés ; - la conformité à des codes de conduite approuvés est prise en compte (Article 35(8)). | ☑ | 1. Étude du contexte |
| <p>La nécessité et la proportionnalité sont évaluées (Article 35(7)(b)) :</p> <ul style="list-style-type: none"> - les mesures envisagées pour se conformer au Règlement sont déterminées (Article 35(7)(d) et considérant 90) en tenant compte : <ul style="list-style-type: none"> - des mesures contribuant à la proportionnalité et à la nécessité du traitement, sur la base de : <ul style="list-style-type: none"> - une(des) finalité(s) déterminée(s), explicite(s) et légitime(s) (Article 5(1)(b)); - la licéité du traitement (Article 6); - des données adéquates, pertinentes et limitées à ce qui est nécessaire (Article 5(1)(c)); - une durée de conservation limitée (Article 5(1)(e)); - des mesures contribuant aux droits des personnes concernées : <ul style="list-style-type: none"> - l'information des personnes concernées (Articles 12, 13 et 14); - le droit d'accès et à la portabilité (Articles 15 et 20) ; - les droits de rectification et à l'effacement (Articles 16 et 17); - les droits d'opposition et à la limitation du traitement (Articles 16 et 21); - les sous-traitants (Article 28); - les mesures encadrant le(s) transfert(s) internationaux (Chapitre V). | ☑ | 2. Étude des principes fondamentaux |
| <p>Les risques sur les droits et libertés des personnes concernées sont gérés (Article 35(7)(c)):</p> <ul style="list-style-type: none"> - l'origine, la nature, la particularité et la gravité des risques sont appréciées (cf. considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime, modification non désirée et disparition de données), du point de vue des personnes concernées : <ul style="list-style-type: none"> - les sources de risques sont prises en compte (considérant 90) ; - les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'accès illégitime, de modification non désirée et de disparition de données ; - les menaces qui pourraient mener à un accès illégitime, une modification non désirée et une disparition de données sont identifiées ; - la vraisemblance et la gravité sont estimées (considérant 90) ; - les mesures envisagées pour traiter ces risques sont déterminées (Article 35(7)(d) et considérant 90). | ☑ | 3. Étude des risques liés à la sécurité des données |
| <p>Les parties intéressées sont impliquées :</p> <ul style="list-style-type: none"> - le conseil du délégué à la protection des données est demandé (Article 35(2)) ; - l'avis des personnes concernées ou de leurs représentants sont demandés (Article 35(9)). | ☑ | 4. Validation du PIA |